NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 8000.4A
Effective Date:
December 16, 2008
Expiration Date:
December 16, 2013

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: Agency Risk Management Procedural Requirements

Responsible Office: Office of Safety and Mission Assurance

Chapter 3. Requirements for Risk Management

As discussed in Chapter 2, Roles and Responsibilities, the applicability of these requirements to individual organizational units is determined by the management of the organizational hierarchy within which those organizational units function.

3.1. General Risk Management Requirements

3.1.1 The manager of each organizational unit shall:

a. Ensure that the RIDM and CRM processes are implemented within the unit (Requirement 59253.

b. Designate the risk manager(s) for that unit (Requirement 59254).

> *Note: The role of risk manager may not need to be a full-time position. The amount of time devoted to performing the risk manager function is commensurate with the size of the organizational unit and the scope of risk that applies to the organizational unit. In addition, rather than assigning individual risk managers to subordinate organizational units, organizational unit managers may choose to incorporate all or some of the subordinate organizational units under the control of a single risk manager provided that the single risk manager has access to each of the subordinate activities for the purpose of performing the risk management function. The intent of the requirement is to assure that the function is performed, not to constrain how the organizational unit manager assigns responsibilities.*

c. Ensure that the designated risk manager has experience in risk and decision analysis

and in the CRM process (Requirement 59256).

d. Ensure that key decisions of the organizational unit are risk-informed (Requirement 59257).

Note: Examples of key decisions include: Architecture and design decisions, make-buy decisions, source selection in major procurements, budget reallocation (allocation of reserves).

e. Ensure that risks are identified and analyzed in relation to the performance requirements for each acquisition of the organizational unit and risk analysis results are used to inform the source selection (Requirement 59259)

Note: Appendix C contains good practices for procurement/contract risk management.

f. Ensure, and concur in, the definition of elevation thresholds to be applied by lower-level organizational units reporting to the unit (Requirement 59261).

g. Ensure that cross-cutting risks and interdependencies between risks are properly identified as cross-cutting and either managed within the unit or elevated (Requirement 59262).

Note: In general, the cross-cutting character of a given risk is best determined by an organizational unit at a level above the level at which that risk is first identified.

Note: Tools of KM are expected to be particularly valuable in this regard.

h. Coordinate the management of cross-cutting risks being managed within the unit with other involved organizational units; e.g., Centers, Mission Support Offices, programs, projects (Requirement 59265).

i. Ensure that dissenting opinions arising during risk management decision making are handled through the dissenting opinion process as defined in NPR 7120.5D (Requirement 59266).

j. Ensure that risk management activities of the organizational unit support, and are consistent with, ongoing internal control activities defined in NPD 1200.1 (Requirement 59267).

3.1.2 The risk manager of each organizational unit shall:

a. Facilitate the implementation of RIDM and CRM (Requirement 59269).

b. Ensure that appropriate training is provided to organizational unit staff on risk management policies, tools, and processes, and ensure that the training material is consistent with the requirements of this NPR (Requirement 59270).

c. Ensure the development of a Risk Management Plan that:

(1) Is integrated into the Systems Engineering Management Plan (SEMP), when applicable per NPR 7123.1 (Requirement 59293)

for program/project units).

Note: In the case of organizational units that do not have a SEMP, the Risk Management Plan is a stand-alone document or a part of program/project plans.

(2) Explicitly addresses safety, technical, cost, and schedule risks (Requirement 59295).

(3) Delineates the organizational unit's approach for applying RIDM and CRM within a graded approach (Requirement 59296).

Note: A "graded approach" applies risk management processes at a level of detail and rigor that adds value without unnecessary expenditure of unit resources.

(4) For each performance requirement, documents, or indicates by reference, whether its associated risks (including the aggregate risk) are to be assessed quantitatively or qualitatively and provides a rationale for cases where it is only feasible to assess the risk qualitatively (Requirement 59298).

(5) Defines categories for likelihood and consequence severity, when risk characterization requires specifying risks in terms of such categories (Requirement 59299).

(6) Identifies stakeholders, such as Risk Review Boards, to participate in deliberations regarding the disposition of risks (Requirement 59300).

(7) Establishes risk acceptability criteria, thresholds, and elevation protocols (the specific conditions under which a risk management decision must be elevated through management to the next higher level) (Requirement 59301).

Note: A "risk acceptability criterion" is a rule for determining whether a given organizational unit has the authority to decide to accept a risk.

(8) Establishes risk communication protocols between management levels, including the frequency and content of reporting, as well as identification of entities that will receive risk tracking data from the unit's risk management activity (Requirement 59303)

Note 1. This communication may be accomplished using standard reporting templates, including risk matrices, whose formulation and interpretation are agreed between the affected units, recognizing that risk communication inputs to any given level (e.g., the program level) from different units (e.g., projects) should be defined consistently, in order to support decision-making at that level.

Note 2. In general, elevation protocols and communication protocols are specific to levels and units. A risk that requires elevation from one level to the next may well be manageable at the higher level, since the unit at that level has more flexibility and authority. The overall effectiveness of the risk management effort depends on the proper assignment of risk acceptability criteria and thresholds.

Note 3. For Center support units, protocols are needed for reporting risks to affected program/project units.

(9) Delineates the processes for coordination of risk management activities and sharing of risk information with other affected organizational units (Requirement 59307).

(10) Documents the concurrence of the organizational unit management to which the risk manager's organizational unit reports, including its risk reporting requirements (Require (Requirement 59308).

d. Periodically review the risk management plan to ensure its currency (Requirement 59309).

3.2 Requirements for the RIDM Process

The manager of each organizational unit shall:

a. Ensure that performance measures defined for the organizational unit are used for risk analysis of decision alternatives to assist in RIDM (Requirement 59312).

b. Ensure that the bases for performance requirement baselines (or rebaselines) are captured (Requirement 59313).

c. Negotiate institutional support performance requirements with Center support units when required to meet program/project requirements (Requirement 59314)

for program/project units).

d. Ensure that performance measures defined for the organizational unit are used to scope the unit's CRM process (Requirement 59315).

3.3 Requirements for the CRM Process

3.3.1 General Requirements

The risk manager shall:

a. Implement the CRM process (as defined in this NPR in paragraph 3.3.2) (see also Figure 4 and associated discussion) (Requirement 59319).

b. Coordinate the unit's CRM process with the CRM processes of organizational units at levels above and below, including contractors if applicable (Requirement 59320).

c. Ensure that risk documentation is maintained in accordance with NPD 1440.6 and NPR 1441.1, and under formal configuration control, with a capability to identify and readily retrieve the current and all archived versions of risk information and the Risk Management Plan (Requirement 59321).

3.3.2 Specific Requirements

3.3.2.1 Identify

a. The risk manager of any given unit shall ensure that the execution of the risk identification step is thorough and consistent with the baseline performance requirements of that unit (Requirement 59324).

b. The risk manager shall ensure that risk analyses performed to support RIDM are used as input to the "Identify" activity of CRM (see paragraphs 3.2.a and 3.2.b) (Requirement 59325).

c. The risk manager shall ensure that the results of risk identification are documented to provide input to the "Analyze" step and to characterize the risks for purposes of tracking (Requirement 59326).

Note: Depending on the type of risk, this documentation will take the form of a "risk statement" or "risk scenario." Each risk statement or scenario is accompanied by a descriptive narrative, which captures the context of the risk by describing the circumstances, contributing factors, uncertainty, range of possible consequences, and related issues (such as what, where, when, how, and why).

3.3.2.2 Analyze

a. The risk manager shall determine the protocols for estimation of the likelihood and magnitude of the consequence components of risks, including the timeframe, uncertainty characterization, and quantification when appropriate, and document these protocols in the Risk Management Plan (Requirement 59329).

Note: The requirement to consider uncertainty is to be implemented in a graded fashion. If uncertainty can be shown to be small based on a simplified (e.g., bounding) analysis, and point estimates of performance measures clearly imply a decision that new information would not change, then detailed uncertainty analysis is unnecessary. Otherwise, some uncertainty analysis is needed to determine whether the expected benefit of the decision is affected significantly by uncertainty. In some cases, it may be beneficial to obtain new evidence to reduce uncertainty, depending on the stakes associated with the decision, the resources needed to reduce uncertainty, and programmatic constraints on uncertainty reduction activities (such as schedule constraints).

b. When a risk management decision is elevated from a lower-level organizational unit, the risk manager shall recalibrate the associated risk with respect to the requirements, thresholds, and priorities that have been established at the higher level, and enter the recalibrated risks into "Plan," "Track," and "Control" activities at the higher level (Requirement 59331).

c. Wherever determined to be feasible (as documented in the Risk Management Plan), the risk manager shall ensure the characterization of aggregate risk through analysis (including uncertainty evaluation), as an input to the decision-making process (Requirement 59332).

d. The risk manager shall ensure that analyzed risks are prioritized and used as input to the "Plan," "Track," and "Control" activities (paragraphs 3.3.2.3 through 3.3.2.5)

(Requirement 59333).

e. The risk manager shall ensure that the results of the "analyze" step are documented and communicated to unit management (Requirement 59334).

3.3.2.3 Plan

a. Each organizational unit manager, supported by the risk manager, shall ensure that decisions made on the disposition of risks (including decisions regarding implementation of control measures) are informed by the risk analysis results and are consistent with the defined thresholds established in paragraph 3.1.2.c.(7) (Requirement 59336).

b. The organizational unit manager shall ensure that only one of the following possible risk dispositions is applied to any given risk and that, depending on the risk disposition, the appropriate requirement, below, is applied (Requirement 59337).

(1) When a decision is made to *accept* a risk, the risk manager shall ensure that each acceptance is clearly documented in their organizational unit's risk database (list), including the assumptions and conditions (risk acceptability criterion) on which the acceptance is based (Requirement 59338).

(2) When a decision is made to *mitigate* a risk, the risk manager shall ensure that a risk mitigation plan is developed and documented in the risk database (list) (including the appropriate parameters that will be tracked to determine the effectiveness of the mitigation) (Requirement 59339).

(3) When a decision is made to *close* a risk, the risk manager shall ensure that the closure rationale is developed, approval of closure is obtained from the unit manager, and that both rationale and management approval are documented in the risk database (Requirement 59340).

(4) When a decision is made to *watch* a risk, the risk manager shall ensure that tracking requirements are developed and documented in the risk database (list). (Requirement 59341).

(5) When additional information is needed to make a decision, the risk manager shall ensure that efforts to *research* a risk (obtain additional information) are documented and tracked in the risk database (list) (Requirement 59342).

(6) When dispositions (1), (2), (3), (4), or (5) above cannot be applied, the organizational unit manager shall *elevate* the decision to the organizational unit management at the next higher level and document the action taken in the risk database (list) (Requirement 59343).

Note: Center support units elevate risks within the Center hierarchy.

c. For "mitigate," "watch," and "research," the organizational unit manager, supported by the risk manager, shall designate an appropriate entity to implement the disposition (Requi (Requirement 59345).

Note: The entity designated to implement the disposition is typically referred to as the "risk owner."

d. The risk manager shall ensure that all risks categorized as "watch" have decision points, dates, milestones, necessary achievements, or goals identified (Requirement 59347).

3.3.2.4 Track

a. The risk manager shall ensure the development and implementation of a process for acquiring and compiling observable data to track the progress of the implementation of risk management decisions (Requirement 59350).

b. The risk manager shall ensure the dissemination of tracking data to entities identified in the Risk Management Plan as recipients of these data (Requirement 59351).

3.3.2.5 Control

a. The risk manager shall ensure the evaluation of tracking data in order to advise its organizational unit management on the status and effectiveness of decisions implemented in paragraph 3.3.2.3.c (Requirement 59353).

b. The organizational unit manager shall provide feedback to affected organizational units, including the sponsoring unit at the next higher level, on any changes in the status of tracked risks such as, but not limited to, acceptance of a risk or changing a mitigation plan (Requirement 59354).

c. Based on the tracking data, in order to control a given risk, the risk owner shall recommend actions to the organizational unit manager and oversee implementation of risk control actions with which the organizational unit manager has concurred (Requiremen (Requirement 59355).

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | AppendixA | AppendixB | AppendixC | ALL |

| NODIS Library | Program Management(8000s) | Search |

DISTRIBUTION:
NODIS